

Serial No. 09/741,411

A. Partyka 20

Claim Amendments

Amend claims 1-20 as follows:

1           1. (Currently Amended) A method of authentication in a telemetry system, said method  
2 comprising:  
3           transmitting, by each of a plurality of transmitters, transmissions intermittently at time intervals  
4 and at a plurality of frequencies independently of any receiver of said transmissions and independently of  
5 any other of said plurality of transmitters, and  
6           holding, by a receiver, simultaneously for each of said plurality of transmitters, data indicative of  
7 an expected frequency and an expected time of at least one future transmission, and  
8           ~~discriminating transmissions based at least in part on at least one of (a) an expected and an actual~~  
9 ~~transmission frequency and (b) an expected and an actual transmission time.~~

10           authenticating transmissions based on an expected and actual transmission frequency and time.

1           2. (Currently Amended) The method of claim 1 wherein ~~said receiver determines authenticity of~~  
2 ~~transmissions based at least in part on said discriminating, said expected transmission frequency~~  
3 ~~comprises estimate for transmitter reference frequency drift.~~

4           3. (Currently Amended) The method of claim 1 wherein ~~each of said plurality of transmitters~~  
5 ~~encrypts data for transmission, and said receiver decrypts received data, said expected transmission time~~  
6 ~~comprises estimate for transmitter time reference drift.~~

1           4. (Currently Amended) The method of claim 3 1 wherein each of said plurality of transmitters  
2 ~~changes encryption key for each of a plurality of transmissions, controls transmission frequency and time~~  
3 ~~between transmissions based on frequency-time pattern that is different for each of said plurality of~~  
4 ~~transmitters.~~

1           5. (Currently Amended) The method of ~~claim 4~~ claim 1 wherein, ~~for each transmitter, said~~  
2 ~~encryption key is determined based on at least one of (a) frequency hopping and (b) time hopping of said~~  
3 ~~each transmitter, each of said plurality of transmitters is for varying encryption key between~~  
4 ~~transmissions.~~

1           6. (Currently Amended) The method of claim 3 5 wherein ~~said transmitter performs modification~~  
2 ~~of at least a portion of said data for transmission with a modifier that is varied for each of a plurality of~~

Serial No. 09/741,411

A. Partyka 20

3 ~~transmissions. said encryption key is varied based on frequency-time pattern for controlling transmission~~  
4 ~~frequency and time between transmissions.~~

1 7. (Currently Amended) The method of claim 6 ~~1~~ wherein, ~~for each transmitter, said modifier is~~  
2 ~~based on at least one of (a) frequency hopping and (b) time hopping of said each transmitter. each of said~~  
3 ~~plurality of transmitters is for verifiable and variable modification of transmitted messages content based~~  
4 ~~on frequency-time pattern for controlling transmission frequency and time between transmissions.~~

1 8. (Currently Amended) A receiver for authenticating telemetry transmissions, said receiver  
2 comprising:

3 logic for holding, simultaneously for each plurality of transmissions, data indicative of an  
4 expected time and an expected frequency of at least one future transmission, wherein each said plurality  
5 of transmissions is transmitted by a different one of a plurality of transmitters, wherein each of said  
6 plurality of transmitters is for transmitting transmissions intermittently at time intervals and at a plurality  
7 of frequencies independently of any equipment that is capable of receiving any of said transmissions from  
8 any of said plurality of transmitters, and

9 circuitry for receiving said transmissions;

10 wherein said receiver is for ~~discriminating transmissions based at least in part on at least one of~~  
11 ~~(a) an expected and an actual transmission frequency and (b) an expected and an actual transmission time.~~  
12 authenticating transmissions based on an expected and actual transmission frequency and time.

1 9. (Currently Amended) The receiver of claim 8 wherein ~~said receiver is for determining~~  
2 ~~authenticity of transmissions based at least in part on said discriminating. said expected transmission~~  
3 frequency comprises estimate for transmitter reference frequency drift.

1 10. (Currently Amended) The receiver of claim 8 wherein ~~said receiver is for decrypting received~~  
2 ~~data encrypted for transmission by each of said plurality of transmitters. said expected transmission time~~  
3 comprises estimate for transmitter time reference drift.

1 11. (Currently Amended) The receiver of claim ~~10~~ 8 wherein ~~said receiver is for using, for each~~  
2 ~~of said plurality of transmitters, a different decryption key for each of a plurality transmissions. frequency~~  
3 and time of transmissions is controlled according to a frequency-time pattern that is different for each of  
4 said plurality of transmitters.

1 12. (Currently Amended) The receiver of claim ~~11~~ 8 wherein said receiver is for determining, ~~for~~  
2 ~~each of said plurality of transmitters, a key for decryption based, at least in part, on said data indicative of~~

Serial No. 09/741,411

A. Partyka 20

3 ~~an expected time and an expected frequency of at least one future transmission, changing decryption key~~  
4 ~~between transmissions based on a frequency-time pattern for controlling frequency and time of~~  
5 ~~transmissions.~~

1 13. (Currently Amended) The receiver of claim 10 ~~8~~ wherein ~~said receiver is for verification, for~~  
2 ~~each of said plurality of transmitters, based on at least a portion of a known content of received data~~  
3 ~~modified by a modifier varied for each of said plurality of transmissions. said receiver, in operation,~~  
4 ~~authenticates transmissions based on verifiable and variable modification of transmission content,~~

1 14. (Currently Amended) The receiver of claim 13 wherein ~~said receiver is for determining, for~~  
2 ~~each of said plurality of transmitters, said modifier based on said data indicative of an expected time and~~  
3 ~~an expected frequency of at least one future transmission. said verifiable modification is based on~~  
4 ~~frequency-time pattern for controlling transmission frequency and time.~~

1 15. (Currently Amended) A frequency hopping telemetry transmitter comprising:  
2 circuit for transmitting transmissions intermittently, at time intervals and at various frequencies,  
3 independently of any receiver of said transmissions, and

4 logic for holding, in operation, ~~upon each of said transmissions, data indicative of (a) a frequency~~  
5 ~~and (b) time of at least one future transmission, wherein said frequency is predictable based on at least~~  
6 ~~one past transmission frequency; providing a predetermined frequency-time pattern for controlling~~  
7 ~~transmission frequency and time between transmissions, and~~

8 wherein said transmitter is for ~~encryption of data for transmission using an encryption key that~~  
9 ~~varies for each of a plurality of said transmissions, varying encryption, for said transmissions, based, at~~  
10 ~~least in part, on said frequency-time pattern.~~

1 16. (Currently Amended) The transmitter of claim 15 wherein ~~said encryption key is determined~~  
2 ~~based, at least in part, on said data indicative of at least one of (a) frequency and (b) time of at least one~~  
3 ~~future transmission; frequency-time pattern is individually selected for said transmitter from a plurality of~~  
4 ~~predetermined patterns.~~

1 17. (Currently Amended) The transmitter of claim 15 wherein ~~said encryption key is varied~~  
2 ~~according to a sequence that is individually selected for said transmitter from a plurality of predetermined~~  
3 ~~sequences; frequency-time pattern is predetermined based on a transmitter identification.~~

1 18. (Currently Amended) A frequency hopping telemetry transmitter comprising:

Serial No. 09/741,411

A. Partyka 20

2 circuit for transmitting transmissions intermittently, at time intervals and at various frequencies,  
3 independently of any receiver of said transmissions, and

4 logic for ~~holding, in operation, upon each of said transmissions, data indicative of (a) a frequency~~  
5 ~~and (b) time of at least one future transmission, wherein said frequency is predictable based on at least~~  
6 ~~one past transmission frequency; providing a predetermined frequency-time pattern for controlling~~  
7 ~~transmission frequency and time between transmissions, and~~

8 wherein said transmitter is for modification of at least a portion of known data for transmission  
9 using a modifier that is varied ~~for each of a plurality of said transmissions; based, at least in part, on said~~  
10 frequency-time pattern.

1 19. (Currently Amended) The transmitter of claim 18 wherein ~~said modifier is determined based,~~  
2 ~~at least in part, on said data indicative of at least one of (a) frequency and (b) time of at least one future~~  
3 ~~transmission; frequency-time pattern is individually selected for said transmitter from a plurality of~~  
4 predetermined patterns.

1 20. (Currently Amended) The transmitter of claim 18 wherein ~~said modifier is varied according to a~~  
2 ~~sequence that is individually selected for said transmitter from a plurality of predetermined sequences;~~  
3 frequency-time pattern is predetermined based on a transmitter identification.